

# Math 557 Oct 31

## Problems on PA and $\text{PA}^-$

### Problem 1

In PA, we can define  $1 := S(0)$ .  
Show that

$$\text{PA} \vdash \forall x (x \cdot 1 = x)$$

### Problem 2: Non-standard models of $\text{PA}^-$

The set  $\mathbb{Z}[X]$  of polynomials in one variable  $X$  with integer coefficients is a commutative ring with the usual operations. One can order this ring by setting for a polynomial  $p = a_n X^n + \dots a_1 X + a_0$  with leading coefficient  $a_n \neq 0$ :

$$a_n X^n + \dots a_1 X + a_0 > 0 : \iff a_n > 0$$

and thus ordering polynomials  $p, q \in \mathbb{Z}[X]$  by  $p < q : \iff q - p > 0$ .

1. Verify that the subset  $\mathbb{Z}[X]^+$  of polynomials  $p \in \mathbb{Z}[X]$  with  $p \geq 0$  is a model of  $\text{PA}^-$ .
2. What does the natural number  $n$  correspond to in  $\mathbb{Z}[X]^+$ ? In other words, what is the interpretation of the constant term  $\underline{n}$ ?
3. Identify an element of  $\mathbb{Z}[X]^+$  that is larger than any “natural number” and thus “infinitely large”.
4. Is  $\mathbb{Z}[X]^+$  a model of PA?

### Problem 3: Overspill

Let  $\mathcal{M} \models \text{PA}$  be non-standard. A **proper cut** in  $\mathcal{M}$  is a set  $I \subsetneq M$  that is an initial segment of  $M$  and closed under successor, e.g. the standard model  $\mathbb{N}$ .

Show that if  $\bar{a} \in M$  and  $\mathcal{M} \models \varphi(b, \bar{a})$  for all  $b \in I$ , then there is  $c > I$  in  $M$  such that  $\mathcal{M} \models \forall x \leq c \varphi(x, \bar{a})$ .

### Take-Home 1

Show that if  $\mathcal{M} \models \text{PA}^-$ , is non-standard, and satisfies the conclusion of the previous problem, then  $\mathcal{M} \models \text{PA}$ .

## Arithmetical Formulas

### Bounded Quantifiers

For terms  $t$  and formulas  $\varphi$  in the language of  $\text{PA}^-$ , we write

$$\begin{aligned} \exists x < t \varphi \text{ for } & \exists x (x < t \wedge \varphi) \\ \forall x < t \varphi \text{ for } & \forall x (x < t \rightarrow \varphi) \end{aligned}$$

and call  $\exists x < t$  and  $\forall x < t$  **bounded quantifiers**.

## Arithmetical Hierarchy

### Definition 1

- $\varphi$  is a  $\Delta_0$ -formula:  $\iff \varphi$  contains at most bounded quantifiers,
- $\varphi$  is a  $\Sigma_1$ -formula:  $\iff \varphi = \exists \vec{x} \psi$  for a  $\Delta_0$ -formula  $\psi$ ,
- $\varphi$  is a  $\Pi_1$ -formula:  $\iff \varphi = \forall \vec{x} \psi$  for a  $\Delta_0$ -formula  $\psi$ .

This is the beginning of the **arithmetical hierarchy**. Setting

$$\Sigma_0 = \Pi_0 = \Delta_0,$$

we can continue:

- $\varphi$  is a  $\Sigma_{n+1}$ -formula  $\iff \varphi = \exists \vec{x} \psi$  for a  $\Pi_n$ -formula  $\psi$ ,
- $\varphi$  is a  $\Pi_{n+1}$ -formula  $\iff \varphi = \forall \vec{x} \psi$  for a  $\Sigma_n$ -formula  $\psi$ .

Thus, a  $\Sigma_3$ -formula has the form  $\exists \vec{x} \forall \vec{y} \exists \vec{z} \psi$ , where  $\psi$  contains at most bounded quantifiers. This means that bounded quantifiers are not counted;  $\Sigma$  or  $\Pi$  indicates whether the formula begins with a (finite) sequence of  $\exists$ -quantifiers or  $\forall$ -quantifiers respectively, and the index counts the quantifier blocks. So it depends less on the number of quantifiers than on the number of quantifier alternations.

In this classification, we do not distinguish between logically equivalent formulas, so that every  $\Pi_n$ -formula for  $n < m$  is also a  $\Sigma_m$ - and  $\Pi_m$ -formula (by simply prefixing the formula with additional quantifiers over variables that do not occur). Thus we can also define the formula classes

$$\Delta_n = \Sigma_n \cap \Pi_n.$$

This gives us the following picture of the **arithmetical hierarchy**:

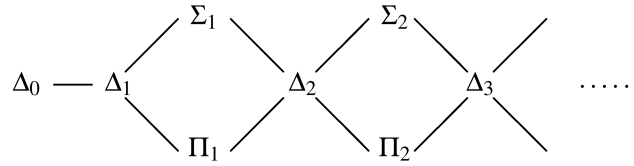


Figure 1: Arithmetical Hierarchy

Many fundamental properties of natural numbers can be expressed using  $\Delta_0$ -formulas, e.g.:

$$x \text{ is irreducible} \iff 1 < x \wedge \forall u < x \forall v < x \neg(u \cdot v = x).$$

### Computability of arithmetical predicates

We will show that the recursive relations coincide with the sets that can be defined by  $\Delta_1$ -formulas, and that the graph of a recursive function can be defined by a  $\Sigma_1$ -formula. We start by showing that  $\Delta_0$ -definable functions are primitive recursive.

### Lemma 2

For every  $\Delta_0$ -formula  $\theta(\vec{v})$ , the relation

$$R(\vec{a}) : \iff \mathbb{N} \models \theta(\vec{a})$$

is primitive recursive.

*Proof.* We show by induction on the height of  $\theta$  that the associated characteristic function

$$c_\theta(\vec{x}) = \begin{cases} 1 & \text{if } \mathbb{N} \models \theta(\vec{x}) \\ 0 & \text{otherwise} \end{cases}$$

is primitive recursive.

First, the functions  $x + 1, x + y, x \cdot y$  are p.r., and thus every term in  $\mathbb{N}$  defines a primitive recursive function. Since the functions  $\text{eq}(x, y) = \overline{\text{sg}}(|x - y|)$  and  $\text{sg}(y \dot{-} x)$  are primitive recursive and the primitive recursive functions are closed under composition, the claim holds for the atomic formulas  $t = s, t < s$ .

For the case of propositional operations, use

$$\begin{aligned} c_{\neg\theta}(\vec{x}) &= 1 \dot{-} c_{\theta}(\vec{x}) \\ c_{\theta \wedge \psi}(\vec{x}) &= c_{\theta}(\vec{x}) \cdot c_{\psi}(\vec{x}) \\ c_{\theta \vee \psi}(\vec{x}) &= \min(c_{\theta}(\vec{x}), c_{\psi}(\vec{x})) \end{aligned}$$

Finally, if  $\psi$  is a  $\Delta_0$ -formula,  $t$  is a term and  $\theta(\vec{x}) = \forall y < t(\vec{x}) \psi(\vec{x}, y)$ , then the claim follows from

$$c_{\theta}(\vec{x}) = \text{eq}(t(\vec{x}), (\mu y < t(\vec{x}) (c_{\psi}(\vec{x}, y) = 0))).$$

One argues similarly in the case of the formula  $\exists y < t(\vec{x}) \psi(\vec{x}, y)$  (or reduces this case to the earlier one using negation).  $\square$

**Remark:** The converse of the above lemma does not hold: there are primitive recursive sets that cannot be defined by any  $\Delta_0$ -formula in the natural numbers.

### Exercise 0.1.

Show that the following relations and functions are primitive recursive.

$$\begin{aligned} &x \text{ divides } y \\ &\text{rem}(x, y) \text{ (remainder when } y \text{ is divided by } x) \\ &x \text{ is prime} \\ &n \mapsto p_n, \text{ where } p_n \text{ is the } n\text{th prime} \end{aligned}$$

## Coding Sequences

The fact that basic number-theoretic functions are primitive recursive allows for primitive recursive encodings of finite sequences of natural numbers by numbers, e.g.

$$(n_0, n_1, \dots, n_k) \quad \text{by} \quad p_0^{n_0+1} \cdot p_1^{n_1+1} \cdot \dots \cdot p_k^{n_k+1}.$$

If we define for  $x, y \in \mathbb{N}$

$$\langle x, y \rangle := \frac{(x + y)(x + y + 1)}{2} + y,$$

we obtain a primitive recursive bijection (pairing function)  $\mathbb{N}^2 \leftrightarrow \mathbb{N}$ . We denote the inverse projections by  $(z)_i$ ,  $i = 0, 1$ , that is,

$$\langle (z)_0, (z)_1 \rangle = z.$$

We can extend this to tuples of arbitrary (but *fixed*) length by iterating:

$$\langle x_1, x_2, \dots, x_k \rangle = \langle x_1, \langle x_2, \dots, x_k \rangle \rangle$$

Using these primitive recursive bijections, we can generally assume functions to be defined on (subsets of)  $\mathbb{N}$ . We can also use it to “compress” quantifiers: For example,  $\exists x \exists y \psi(x, y)$  can be replaced by  $\exists z \psi((z)_0, (z)_1)$  without affecting the arithmetical complexity.

## Take-Home Problems

## Take-Home 2

Show that the *Euler totient function*

$$\phi(x) = \# \text{ of } m \leq x \text{ relatively prime to } x$$

is primitive recursive.

## Take-Home 3

Show that the set of *generalized Mersenne primes*,

$$\left\{ N \text{ prime} : N = \frac{p^n - 1}{p - 1} \text{ for some prime } p \text{ and } n \geq 2 \right\}$$

is primitive recursive.